Conditional Access Best Practices and Policy Examples

Conditional Access enables you to block, allow, or limit access to cloud applications under different circumstances that you define via policy. Think of it as your firewall in the cloud! You can choose to implement some or all these policies,but recommend that you evaluate each one of them mentioned in this book for every new implementation.

**Disclaimers**

The instructions described in thishave been prepared with the utmost care. Each IT environment has its own needs and works with its individual settings and software configurations. No liability can be accepted for any errors or data loss during the execution of the described procedures, scripts, and commands. Please evaluate PowerShell scripts and cmdlets before making any changes in a production environment.

Due to the nature of a modern cloud service, the screenshots depicted herein might be different from the layout and information displayed when you access the service.

© Copyright 2019-2022,

1

Change Log

Some of you have requested a change log for when this document is updated. Here it is.

© Copyright 2019-2022,

2

November 2022

Moved from categorizing by policy type to persona type

January 2022

Updates to naming convention again, added instructions based on the new “Templates” feature.

June 2021

Major updates; revamped policy design and new naming convention

February 2021

Minor updates to *Best practices* section for further clarification

Previous versions

Unknown—was not tracking my changes

Table of Contents

[Conditional Access Best Practices and Policy Examples](#_bookmark0) [1](#_bookmark0)

[Change Log](#_bookmark1) [2](#_bookmark1)

[About Licensing](#_bookmark2) [4](#_bookmark2)

[Conditional Access Best Practices](#_bookmark3) [4](#_bookmark3)

[Users or workload identities](#_bookmark4) [5](#_bookmark4)

[Cloud Apps, User Action, or Auth Context](#_bookmark5) [6](#_bookmark5)

[Conditions](#_bookmark6) [7](#_bookmark6)

[Access Controls](#_bookmark7) [8](#_bookmark7)

[Open vs. Closed policies](#_bookmark8) [10](#_bookmark8)

[Naming convention according to Persona](#_bookmark9) [11](#_bookmark9)

[Example policies using naming convention](#_bookmark10) [12](#_bookmark10)

[Getting Started](#_bookmark11) [13](#_bookmark11)

[Create emergency access accounts](#_bookmark12) [13](#_bookmark12)

[Define trusted locations](#_bookmark13) [14](#_bookmark13)

[Upload Terms of use](#_bookmark14) [15](#_bookmark14)

[Turn off Security Defaults](#_bookmark15) [16](#_bookmark15)

[Building policies from templates](#_bookmark16) [17](#_bookmark16)

[Import policies via PowerShell script](#_bookmark17) [18](#_bookmark17)

[Communicating upcoming changes](#_bookmark18) [19](#_bookmark18)

[Global persona policies](#_bookmark19) [20](#_bookmark19)

[Admin persona policies](#_bookmark20) [21](#_bookmark20)

[Internal persona policies](#_bookmark21) [22](#_bookmark21)

[Guest-specific policy examples](#_bookmark22) [23](#_bookmark22)

[Service account policy examples](#_bookmark23) [24](#_bookmark23)

[Conclusion](#_bookmark24) [24](#_bookmark24)

© Copyright 2019-2022,

3

About Licensing

Conditional Access is available with Azure AD Premium P1 and P2 plans. P1 is included with Microsoft 365 Business Premium, or Microsoft 365 E3 plans, and P2 with Microsoft 365 E5 plans. Every Conditional Access policy have outlined in this guide is compatible with Azure AD Premium P1. There are additional features and capabilities with Azure AD Premium P2, however, they are not necessary for

achieving what consider to be a very strong baseline aligned closely with Zero Trust principles.

Conditional Access Best Practices

Microsoft publishes a list of [Best Practices](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access#follow-best-practices) regarding Conditional Access; it is a short list worth reviewing. have the following advice to add based on my experience:

1)

2)

3)

4)

5)

Implement *closed* policies (assigned to *All users*) to replace Security defaults

Plan out what access scenarios you want to enable for each persona in your organization Use a standardized naming convention

Always exclude your [emergency access account(s)](https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access) from the CA policies; see also: [Plan for disruption](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-resilient-controls)

Special considerations for policies that require device compliance or hybrid Azure AD join:

a)

Complete the initial device onboarding, and verify the status of devices in the cloud *before*

enabling the policies (this is to minimize potential interruption to end users)

recommend open architecture policies (vs. closed) for most small businesses, where you target specific apps like *Office 365* rather than *All cloud apps*

If you want to use closed architecture here, you must exclude the app called *Microsoft Intune*

*Enrollment* or you will be unable to enroll new devices

b)

c)

6)

It is best to enforce *one* access control per policy. While it may be possible to combine access controls in a single policy, it is better for troubleshooting purposes if you keep them apart. For example, rather than requiring MFA *and* device compliance in the same policy, there may be benefit to having two policies (one that accomplishes each outcome): this allows you to troubleshoot issues or make exceptions with the policies independently as needed. Remember that all policies are evaluated simultaneously anyway, so there is no reason not to separate them by access control so you can make granular adjustments. You must balance this against the desire to keep as few policies as possible.

Do not enable any new policies until you have communicated the changes and expected impacts to

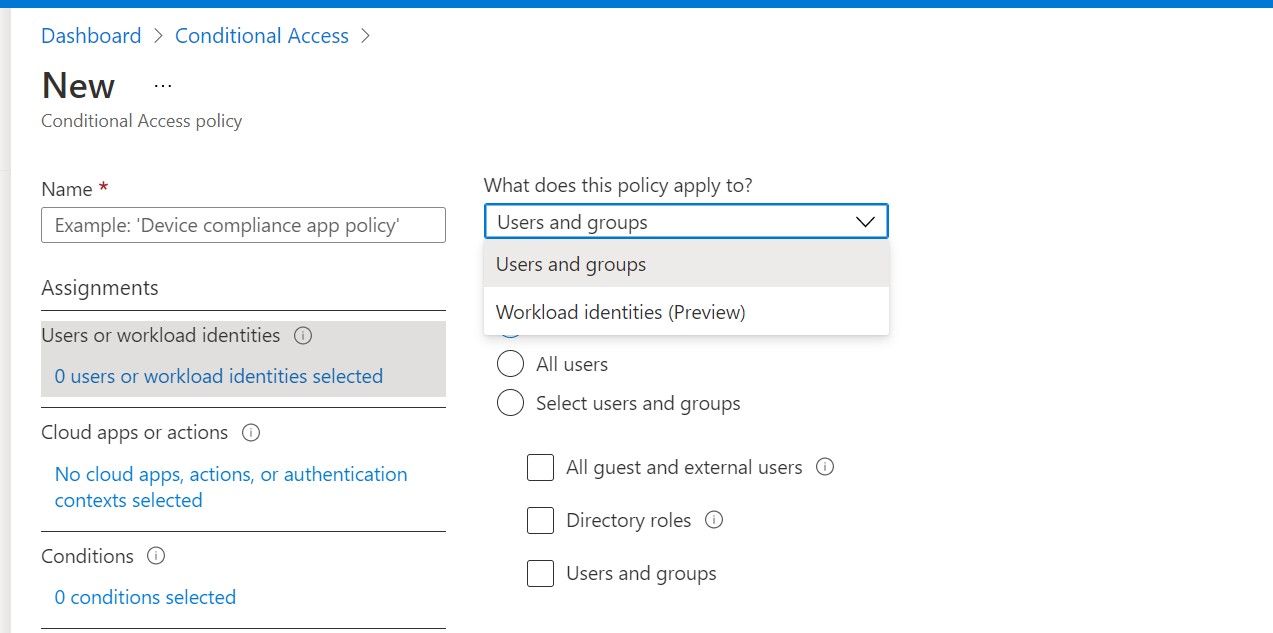
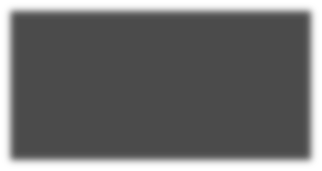
end users in advance. This will help you avoid falling into the pit of end user despair.

7)

As you plan and tweak according to your own implementation, keep the guidelines above in mind. Next, we will cover the innards of CA policies including assignments, protection types, conditions, access controls, and naming conventions.

© Copyright 2019-2022,

4



Users or workload identities

Also known as **personas**, this section of the policy refers to the users or service principals you are targeting with any given Conditional Access policy. Policies are most commonly assigned to one of the

following personas:

**Users and groups**: Most policies will be targeted against users and groups.

•

**All Users**: This is how you target *all users* in a tenant (i.e., Global persona)

**All Guest and external users**: Refers to users outside the organization who are invited to work with corporate applications and data. It is considered a best practice to exclude guests from most standard user policies and target them specifically with the CA policies that you want to enforce.

**Directory roles**: Known as *admin personas*; even though roles such as Global administrator, etc. might already be in the scope of policies covering “*All users*,” it can still be a good practice to scope certain CA policies to admin roles specifically so that they cannot escape the policy, even if another policy is modified or temporarily disabled. **Users and groups:** Usually these are *internal personas*; you can select specific users or security groups here, for example if you wanted to target the *Marketing department* or

*Finance users* specifically.

o

o

o

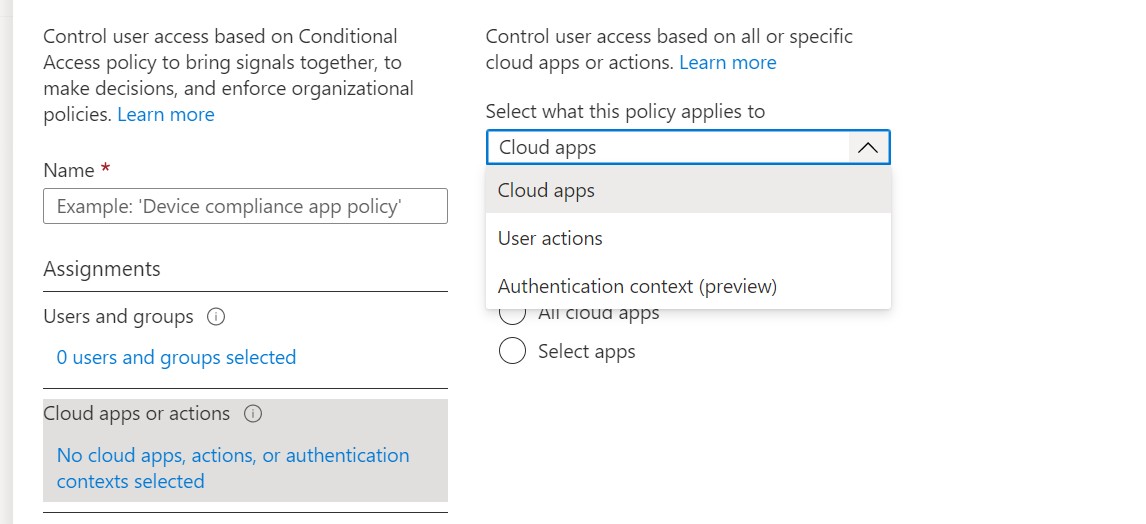
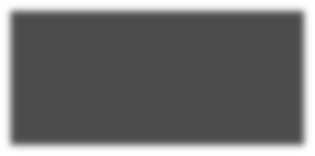
o

•

**Workload identities**: These are application service accounts that do not represent a real human, but rather a service principal.

© Copyright 2019-2022,

5



Cloud Apps, User Action, or Auth Context

Conditional Access policies can be targeted or assigned to different apps, actions, or contexts.

* **Cloud apps:** This is the most common type of policy; use *Cloud apps* to apply your policy to *All*

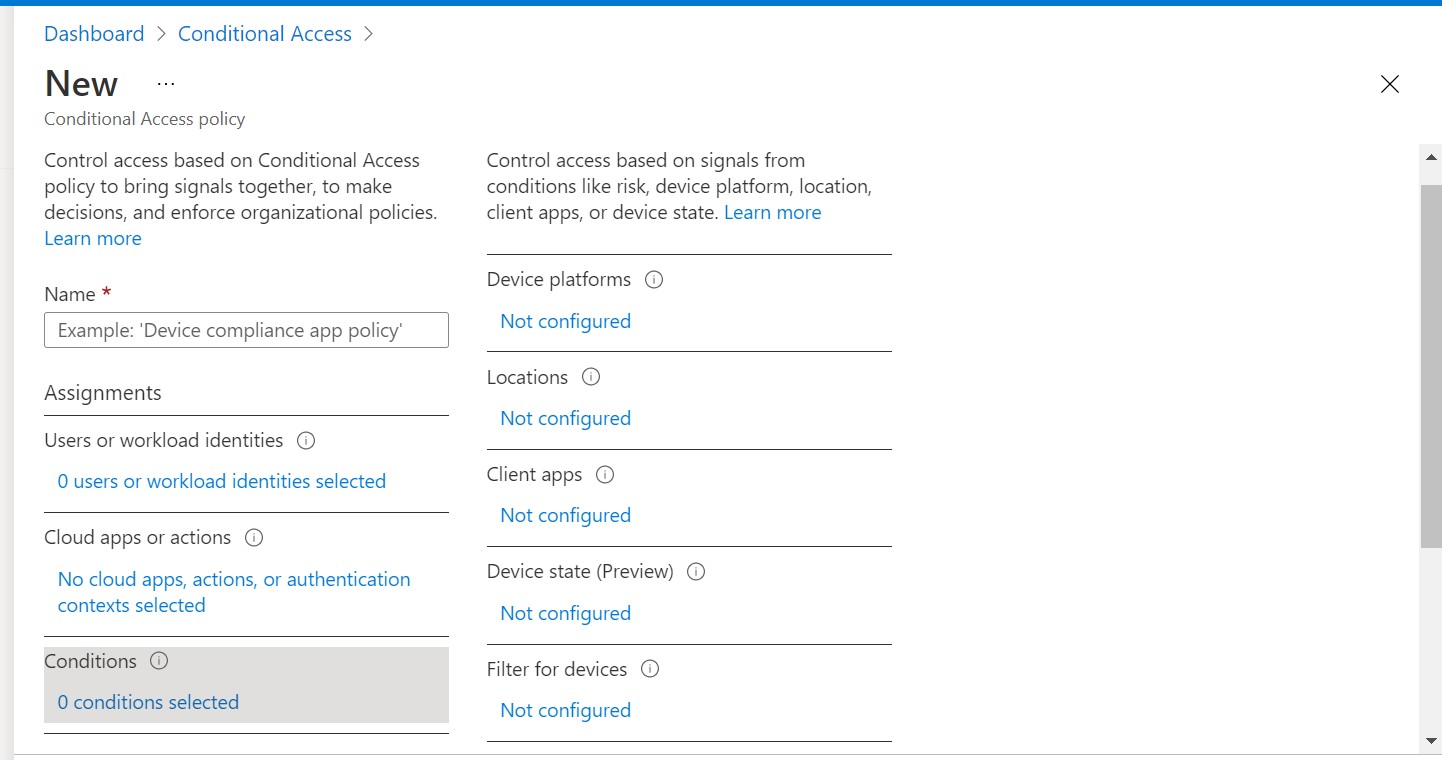
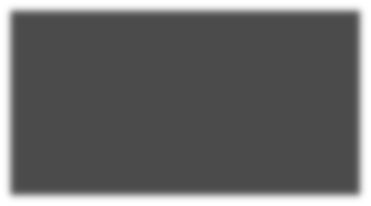
or *specific* cloud applications. Most baseline policies will target either:

* + **All cloud apps:** Targeting *All cloud apps* is also referred to as “closed architecture” policy. Baseline policies like *Block legacy authentication* and *Require multi-factor* are often deployed with closed architecture. Some policies however will require you to *exclude* certain applications.
  + **Select apps > Office 365:** Selecting specific apps is known as an “open architecture” policy. One of the most common open policies is to target *Office 365* for specific access scenarios such as requiring device compliance for accessing company email.
* **User actions:** We currently have two *User actions*:
  + **Register security information:** Use this to apply restrictions to the MFA registration process, such as limiting access to the registration page by trusted locations.
  + **Register or join devices:** When a user registers or joins a device to Azure AD you can require multi-factor authentication.
* **Authentication context:** With [*Authentication context*,](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps#authentication-context-preview) you can create custom triggers within applications like SharePoint or Microsoft Defender for Cloud Apps, where entering a certain area will require additional authentication. This is also known as “Step-up” authentication. For example, you are challenged for MFA when you try to enter a more sensitive area. personally have not found a use for this feature, and instead stick to my baseline policies (already require

MFA and device compliance for most “Standard user” access scenarios anyway).

© Copyright 2019-2022,

6



Conditions

Conditions allow us to “qualify” or “narrow down” our policies further. For example, you can specify conditions that ensure the policy only applies to specific device platforms like iOS and Android. This allows you to deliver a different sign-in experience or result based on attributes other than user identity

and group membership.

**Device platforms**: Use this if your policy should only apply to a specific OS such as Windows or macOS. Common examples include requiring MAM or MDM for mobile devices or requiring Hybrid Azure AD join for Windows devices.

**Locations**: Most often used to exclude trusted locations from a policy, or to block access from specific regions or countries (you have to define [named locations](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition) before you can use this condition).

**Client apps**: Used to target Browser experiences or Mobile app and Desktop client experiences. Also used to block legacy authentication clients.

**Filter for devices**: You can target devices based on attributes such as whether the device is Personal or Company-owned, or whether it is Azure AD Registered, Joined, or Hybrid Joined, or

whether it is compliant with policies in Microsoft Endpoint Manager, etc.

•

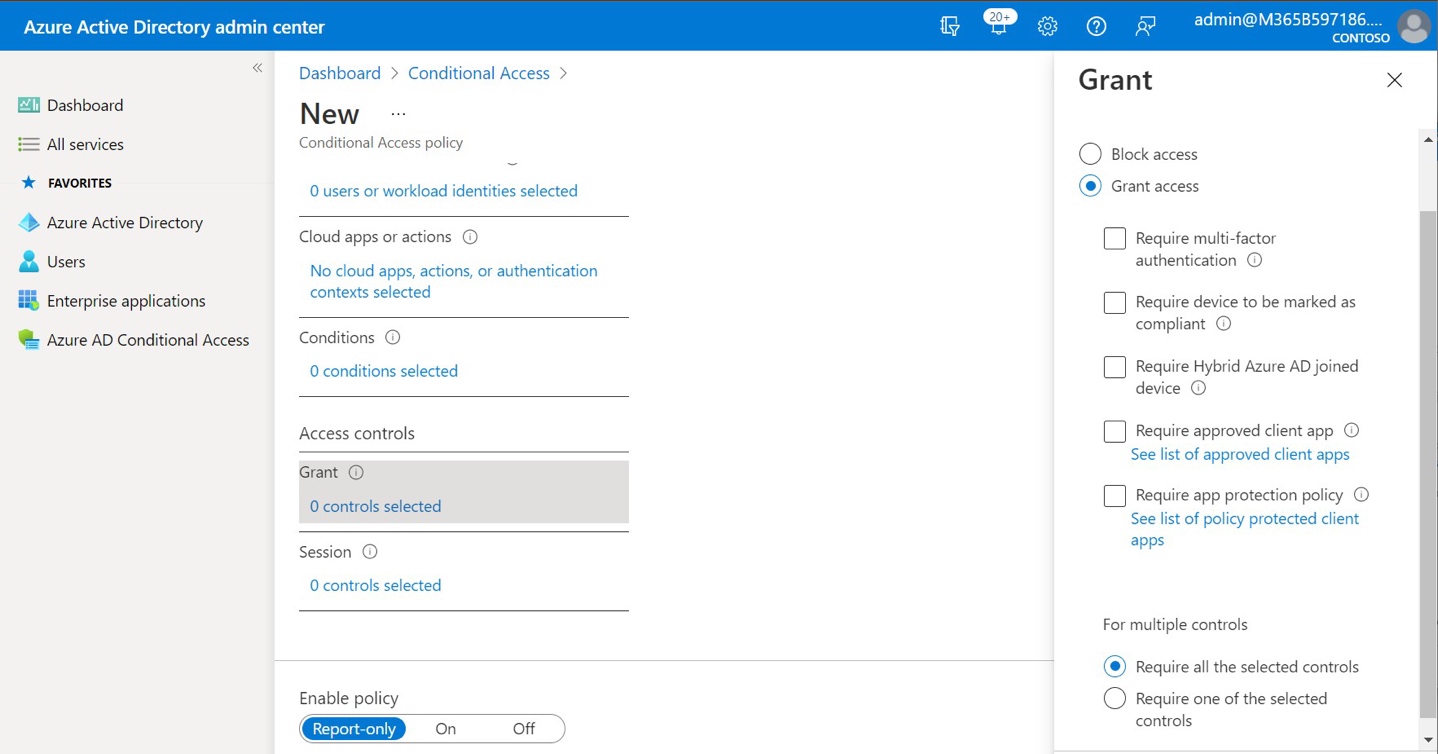
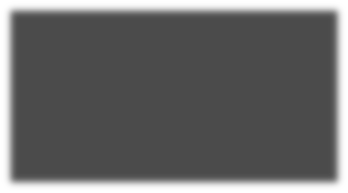
•

•

•

© Copyright 2019-2022,

7



Access Controls

Conditions set up the “IF” and Access controls say, “THEN.” Here we decide what outcomes we desire if the policy conditions are met. There are two types of access controls. Starting with **Grant/Block**:

•

•

**Block access**: Just like it sounds, if selected, access will be denied when conditions are met

**Grant access**: Access is granted when one or more of the following requirements is met:

**Require multi-factor authentication**: User must present a strong authentication method (e.g., Windows Hello, or Microsoft Authenticator app).

**Require device to be marked as compliant**: Device must be enrolled and evaluated by Endpoint Manager compliance policies. Applies to Windows, macOS, iOS, and Android. **Require Hybrid Azure AD joined device**: Applies only to Windows devices; this control is often selected along with the compliant device requirement, with the selection “Require *one* of the selected controls.” These two access controls together basically say “Require devices to be managed” or in other words “Block unmanaged devices.” **Require approved client app**: Only applies to iOS and Android, and only applies to supported (Microsoft) apps such as Office 365. Often combined with the next control.

**Require app protection policy**: Only applies to iOS and Android. Apps must be protected with app protection policies in Endpoint Manager. Also known as MAM. **Require terms of use**: Once you set up terms of use, you can choose to enforce

acceptance of the terms as an access control. More on this in a later section.

o

o

o

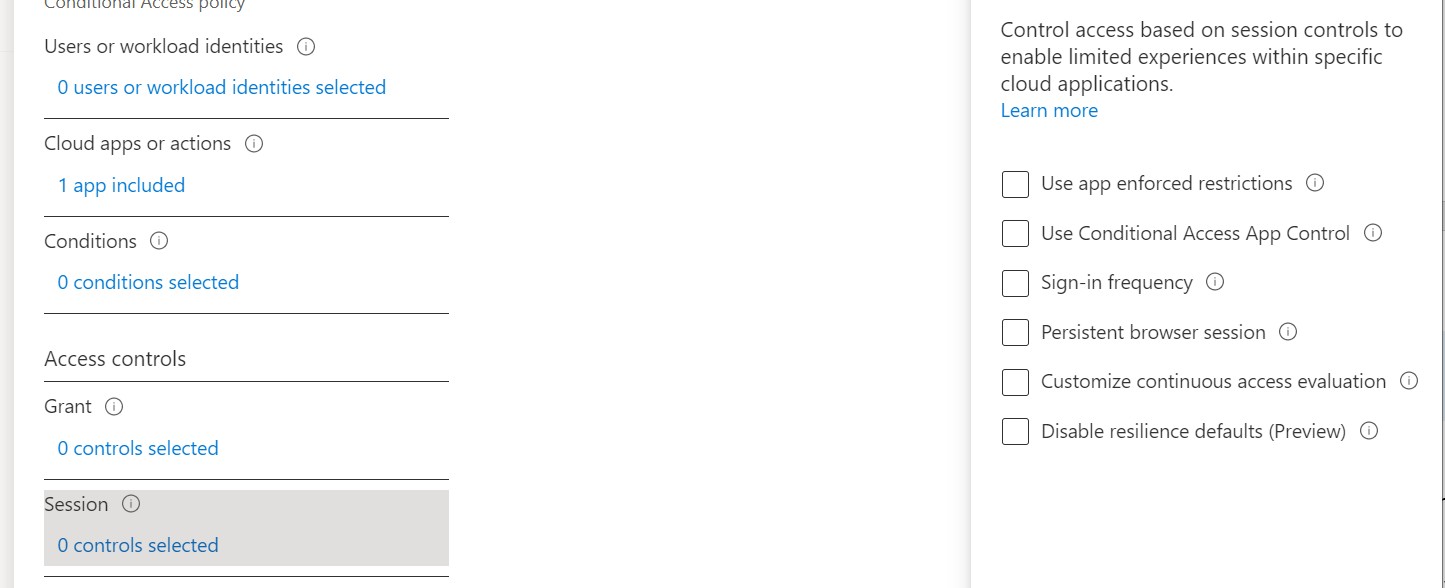
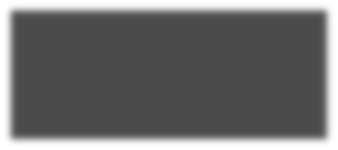
o

o

o

© Copyright 2019-2022,

8



**Require *all* of the selected controls**: If you select more than one access control, then all must be true in order to grant access.

**Require *one* of the selected controls**: If you select more than one access control, then only one

must be met in order to grant access.

•

•

Moving on to **Session controls**:

**Use app enforced restrictions**: Only Office 365 Exchange Online and SharePoint Online have this option. When it is enabled, unmanaged devices cannot download or sync data to the local device. This also requires configuration in Exchange Online and SharePoint Online to take effect. More on this in a later section.

**Use Conditional Access App Control**: This is an integration that works with Microsoft Defender for Cloud Apps. Once enabled, you can create more granular security policies in MDCA. [Read](https://docs.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad) [more here.](https://docs.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad)

**Sign-in frequency**: Require users to sign-in more frequently (personally dislike messing with this and prefer to leave the default behavior; stuff like MFA and device compliance is more important than sign-in frequency). [Read more here.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime#user-sign-in-frequency)

**Persistent browser session**: You know that prompt that asks if you want to stay signed in? You can make it go away. Especially for guests or unmanaged devices, it is a good idea to disable persistent sessions. [Read more here.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime#persistence-of-browsing-sessions)

**Customize continuous access evaluation**: It used to be that you had to turn this feature on, and it was considered a best practice to do so. This is now on by default, so this option exists to disable it (or enforce it strictly) which is not recommended. [Read more here.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation)

**Disable resilience defaults**: Another option that allows us to disable something that ought not

be disabled in most cases. [Read more here.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/resilience-defaults)

•

•

•

•

•

•

© Copyright 2019-2022,

9

Open vs. Closed policies

Conditional Access policies can be *Open* or *Closed*.

**Closed** means scoping policies to “**All Cloud Apps**.” Here is an example of a **Global** persona policy that is also **Closed**:

* Users or workload identities: **All users**
* Cloud apps or actions: **All cloud apps**
* Conditions: None
* Access controls: Require multi-factor authentication

The closed architecture approach is preferred as it is better aligned to a “Zero Trust” security model, meaning that it leaves less room for errors or blind spots. However, there may be additional considerations and impacts with global policies, since not all apps will support every access control.

**Open** means that you are scoping your policies to specific applications such as “Office 365 apps.” In this case you are asking the CA policy to affect a more targeted outcome or access scenario. Example of an

**Internal** persona policy that is open architecture:

Users or workload identities: **All employees** Cloud apps or actions: **Office 365** Conditions: Device platforms: iOS, Android

Access controls: Require device to be marked as compliant

•

•

•

•

Also note that it is totally acceptable to have a mixture of *closed* and *open* policies in your environment. In some cases, you want to apply policies globally (e.g., Require MFA), and in others you may want to be more targeted in order to affect a specific experience (for example, to control guest experiences differently than standard user experiences, or to apply more protection to data in a specific application

like Office 365).

© Copyright 2019-2022,

10

Naming convention according to Persona

When you name your Conditional Access policies, it is a good idea to follow a standard naming convention that is both logical and well documented. For example, policies can be categorized according to the “personas” which are being targeted; personas can be “numbered” or “tagged,” and

this “tag” can make it easier to organize, manage, and sort your policies according to purpose.

Each persona has a specific set of access requirements that you want to enforce. For example, external personas may have different requirements than internal ones. You may have more stringent requirements for administrator accounts, and application personas might be location-bound.

This is just one possible breakdown; some folks choose to expand on this concept or adopt their own practices altogether. have changed my naming convention several times over the years, and yes, it is somewhat arbitrary. But really do like the simplicity of a numbering system (rather than trying to identify policy purpose with more words/text). The key is maintaining consistency across all the tenants you manage, so that it is easy for your team to orient quickly during support requests, and to make

long-term versioning/change requests easier.

© Copyright 2019-2022,

11

**Policy numbers**

**Persona type**

**Description / examples**

CA001 – CA099

Global policies

Policies that apply to **All users** regardless of persona

CA101 – CA199

Admin personas

Policies that only apply to **administrator roles**

CA201 – CA299

Internal personas

Policies that apply to **internal users** (i.e., employees)

CA301 – CA399

External personas

Policies that target to **guests and external users**

CA401 – CA499

Apps or service accounts

Either **service accounts** or **service principals**

Example policies using naming convention

You are free to choose your own naming convention, but have used the following format in this guide: Policy number: Description of policy (Open targeting if applicable)

Examples:

\**These four policies together replace the Security defaults feature*

Another option is to prefix a version number in brackets, e.g., *[v1.0] CA001: Block legacy authentication.*

That way, if you develop a baseline and then add different iterations afterward, the version number can help you track changes across tenants over time.

© Copyright 2019-2022,

12

**Personas**

**Policy Name**

**Global**

CA001:

Block legacy authentication\*

CA002:

Block access for unsupported device platforms

CA003:

Require MFA for Azure management\*

CA004:

Require MFA to register or join devices

CA005:

No persistent browser session for unmanaged devices

CA006:

Block access from unsupported countries

**Admins**

CA101:

Require MFA for admins\*

CA102:

No persistent browser session for admins

CA103:

Require managed devices for admins

**Internals**

CA201:

Require MFA or compliant device for internal users\*

CA202:

Securing security info registration

CA203:

Require MAM or MDM for mobile device access

(Office 365)

CA204:

Require compliant device or hybrid join for desktop access

(Office 365)

CA205:

Block downloads on unmanaged browsers and devices

(Office 365)

CA206:

Require terms of use for standard users

**Externals / Guests**

CA301:

Block guest access to unsupported apps

CA302:

Require MFA for guest users

CA303:

Require terms of use for guest users

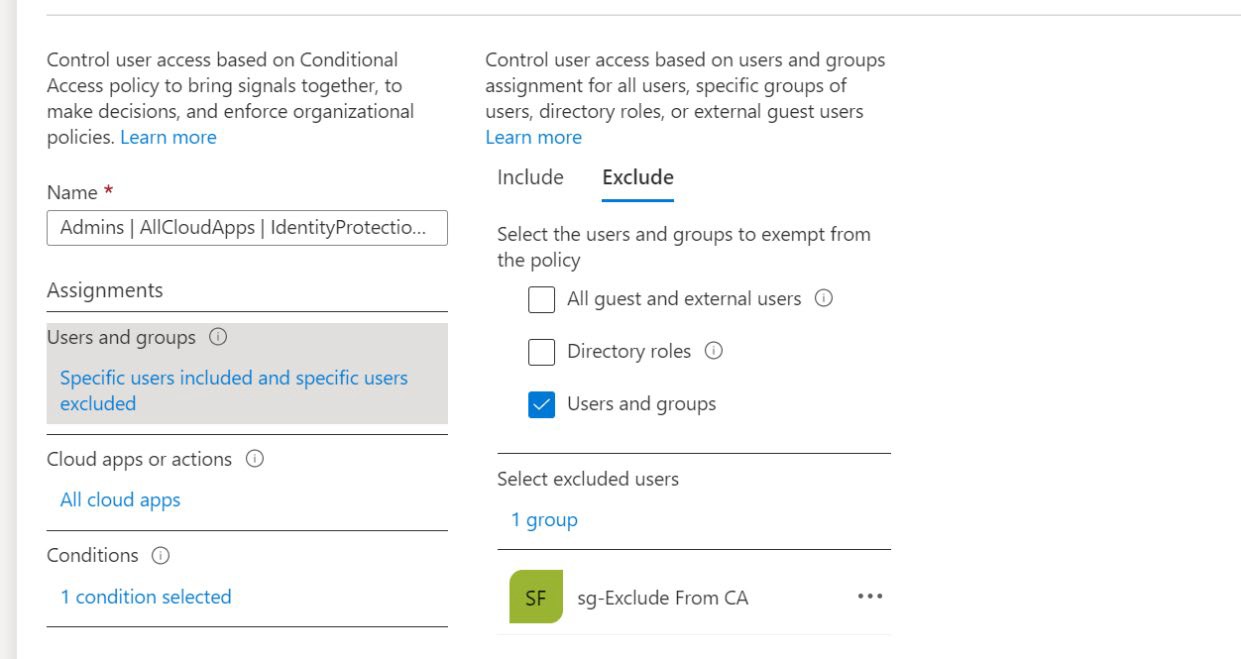
**Applications & Services**

CA401:

Block service account access to unsupported apps

CA402:

Block service principal access from untrusted locations



Getting Started

You should plan to follow each of the steps below (in order) for the best results:

1)

2)

3)

4)

5)

6)

Create emergency access account(s) which are excluded from all policies Define any named locations you intend to use

Turn off Security defaults

Build or import your baseline policies Communicate upcoming changes

Enable the policies per your communications

Create emergency access accounts

As mentioned, you should exclude at least one [emergency access “break glass” admin account](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access) from all Conditional access policies. usually start by creating a security group called “sg-Exclude from CA” and then place my emergency access account(s) into that group.

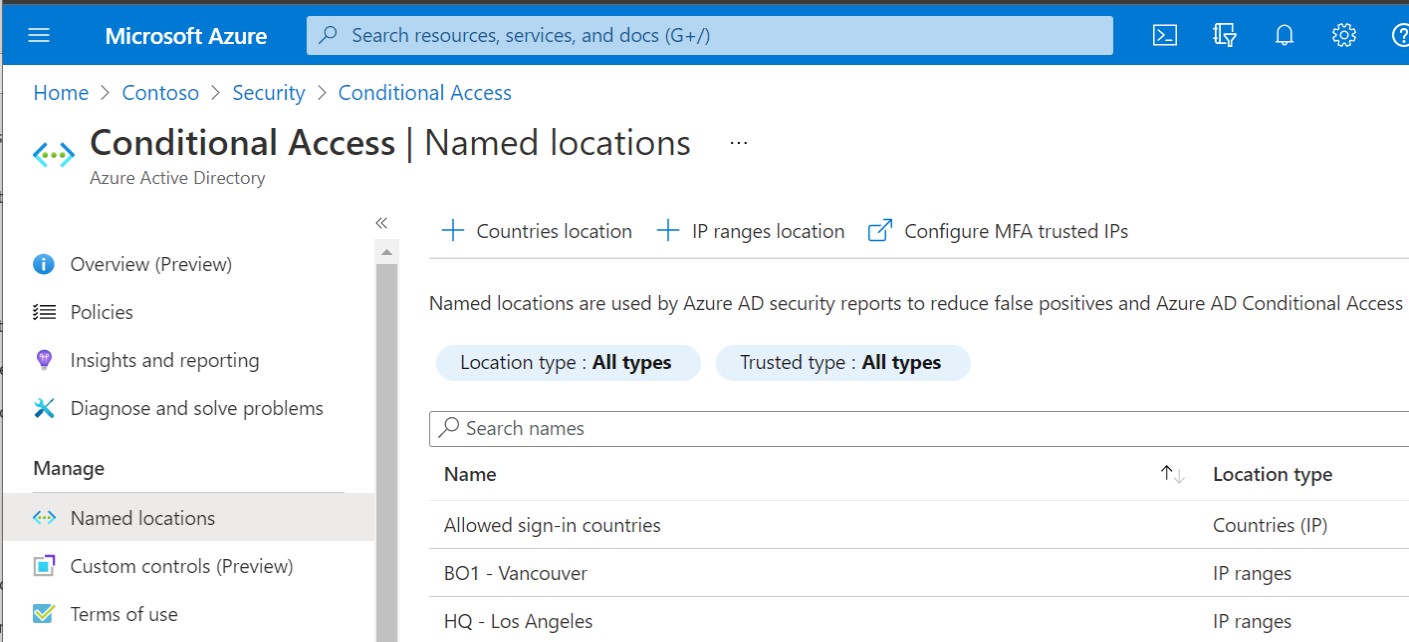
The security group will be added to each Conditional Access policy under **Exclude** in the **User and group** assignments.

*Note: If you deploy the Microsoft templates, then the account you use to create those policies is automatically excluded; if you use my scripts, then the script will check for*

*and create a security group which you can then populate.*

© Copyright 2019-2022,

13



Define trusted locations

The next step is to define our trusted locations. Go to **Azure Active Directory > Conditional access**

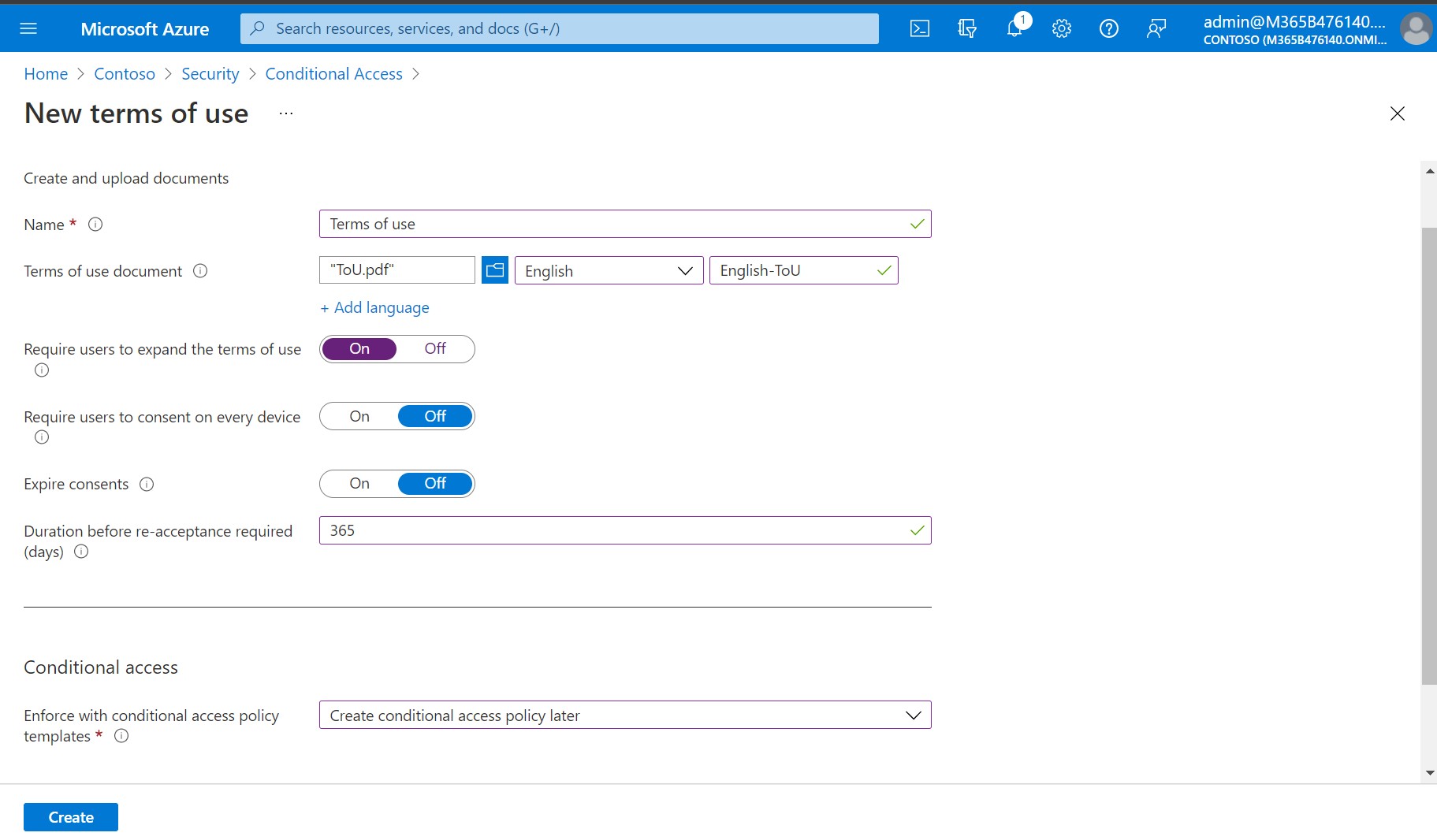
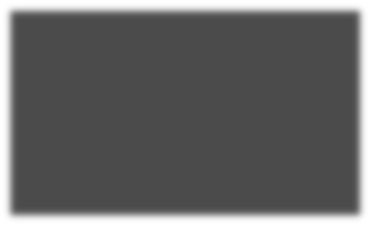
and choose **Named locations**.

You can add a **Countries location** (e.g., Allowed sign-in countries), and/or **IP ranges location**, which are locations that represent corporate offices (normally marked as “trusted” locations. Certain policies can be configured to exclude these locations. For instance, you can block access from all locations

except for the approved sign-in countries.

© Copyright 2019-2022,

14



Upload Terms of use

Some organizations will want to display a “Terms of Use” document to their end users, which is accepted annually or semi-annually.

If that describes your situation, navigate to **Azure AD > Security > Conditional access** and click on

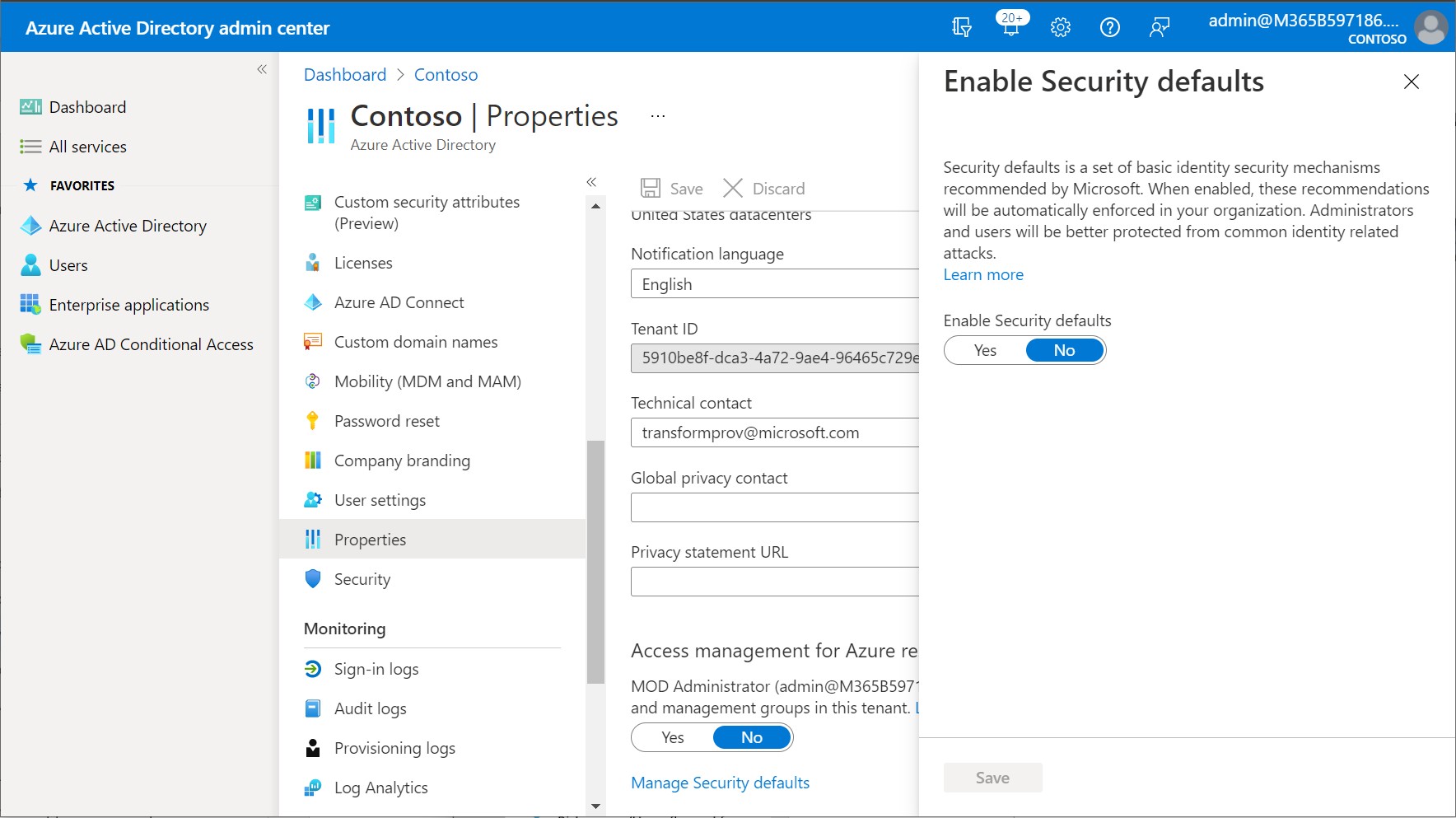
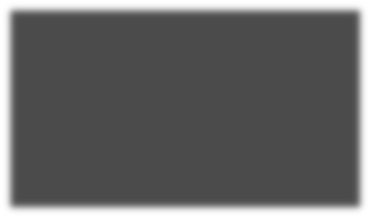
**Terms of use**. Click **New terms**.

Make selections similar to those pictured here, uploading your own terms of use (note: use 24-point font for best display on mobile devices), or make your own custom selections and click **Create**. You can also create multiple terms of use if you have different terms targeted to different personas (e.g., Guests,

Internals, Admins, etc.)

© Copyright 2019-2022,

15



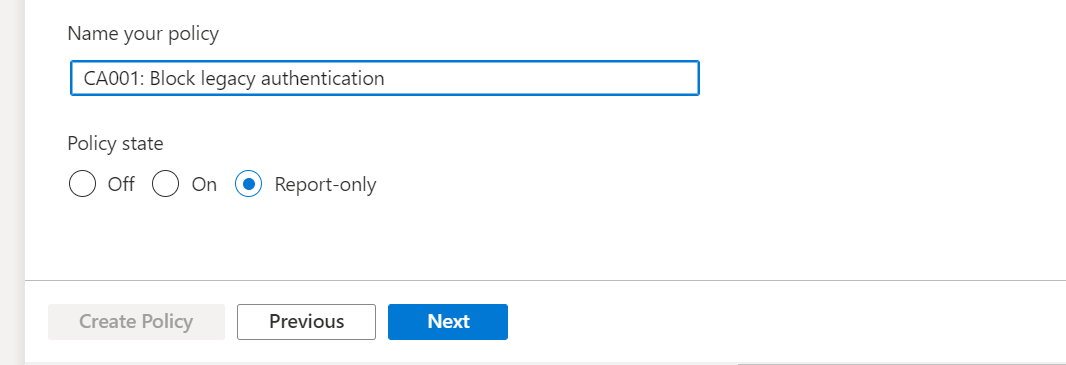
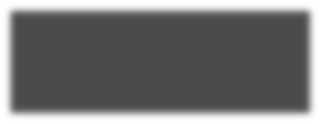
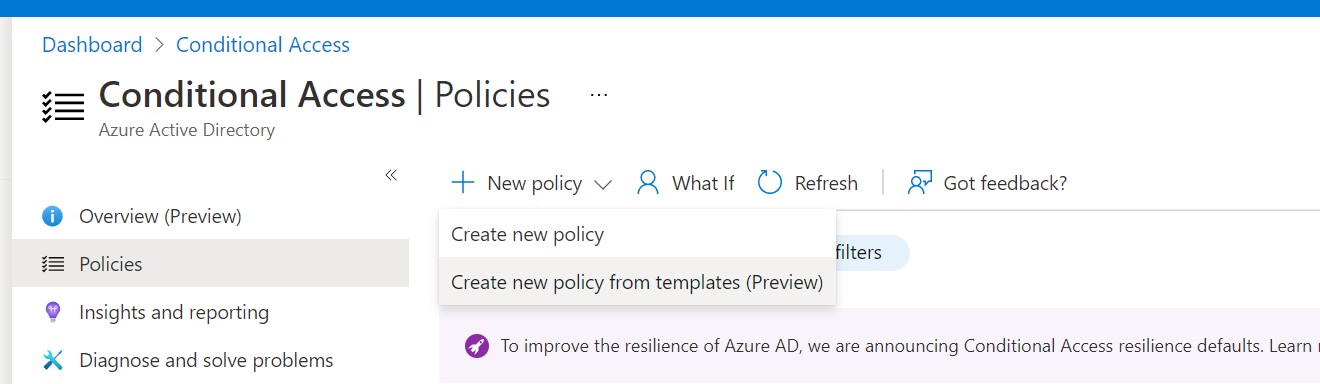
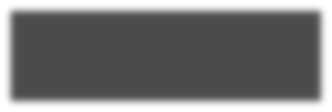
Turn off Security Defaults

Before we begin creating our first policies, we must discuss the [**Security Defaults**.](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-security-defaults) Navigate to **Azure AD admin center > Properties > Manage Security defaults**.

It is important to note that you cannot enable the Security Defaults feature if you are going to deploy custom Conditional Access policies. In fact, the presence of even one custom policy will prevent you from enabling this feature. Set **Enable Security defaults** to **No**.

© Copyright 2019-2022,

16



Building policies from templates

Microsoft provides a number of [templates](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common) that you can use to quickly deploy the most important baseline policies. If you are going to use this method, then login to the Azure AD portal with your emergency admin account. The account that you use to deploy each policy is automatically excluded.

Navigate to **Azure Active Directory > Security > Conditional Access**. From the **New policy**

dropdown menu, choose **Create new policy from templates**.

Start with **Identities** and click **Next**. Here we find several of the recommended baseline policies. Simply select one of the templates, for example **Block legacy authentication**. You can change the name of the

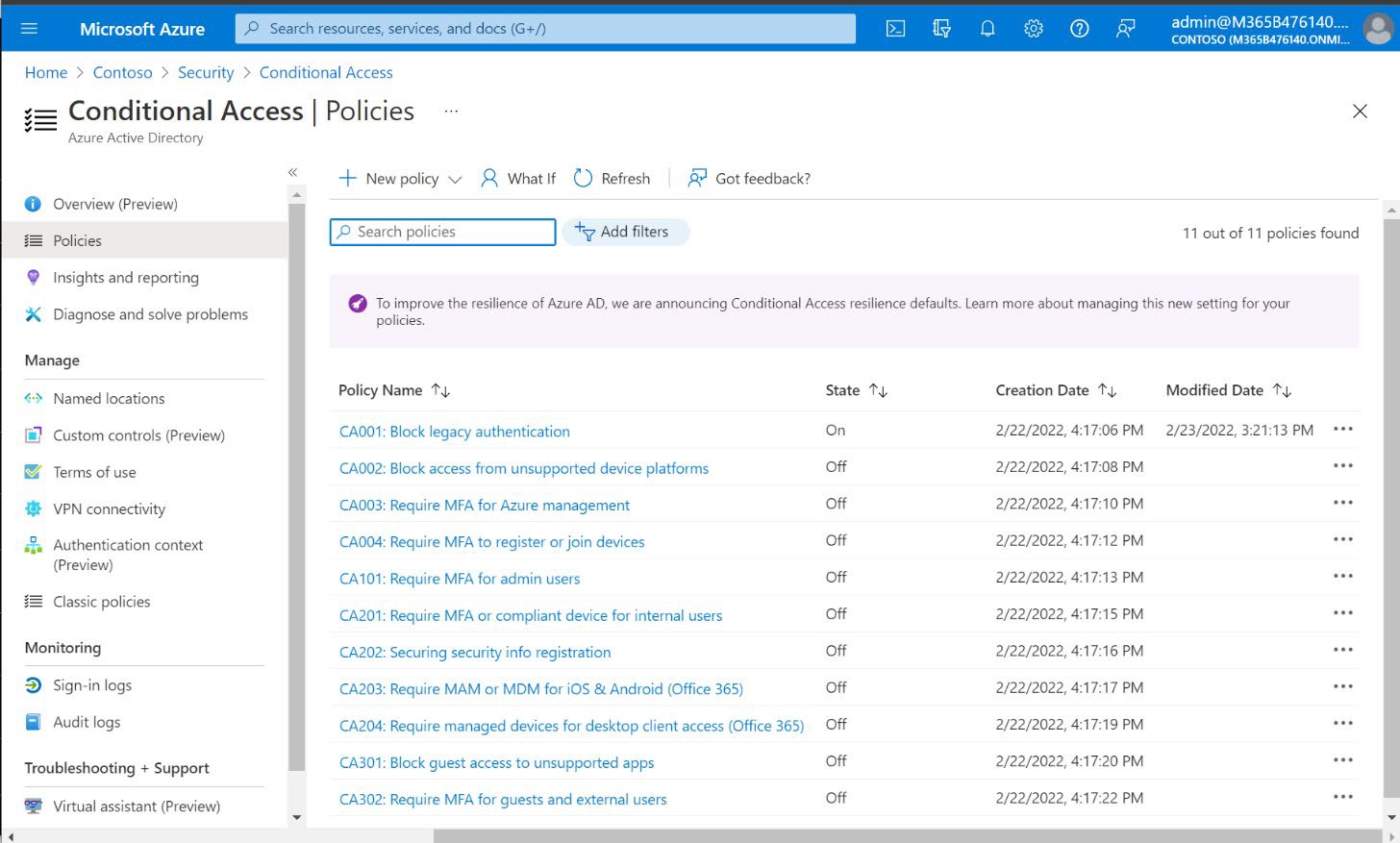
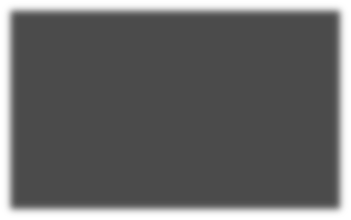
policy to match your own naming convention (for example if you have a preferred numbering scheme).

At the bottom of the page, choose the policy state: **On** right away, or leave it in **Report-only** mode (default). **Next** to review and **Create policy**. You can repeat these steps for other policies, paying

attention to the naming scheme and policy state that makes the most sense for your deployment.

© Copyright 2019-2022,

17



Import policies via PowerShell script

The most important policies that describe in this resource are available in my [GitHub repository.](https://github.com/vanvfields/Microsoft-365)

* [**Install-ITPMBaselineCAPolicies.ps1**:](https://github.com/vanvfields/Microsoft-365/blob/master/Azure%20AD/Install-ITPMBaselineCAPolicies.ps1) Run this script to import the core policies that use with all of my customers.

You may need to install the [Azure AD Preview](https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-adv2?view=azureadps-2.0&installing-the-azure-ad-module) module and set your execution policy to run the scripts. Review the imported policies by navigating to [Azure AD > Security > Conditional Access.](https://aad.portal.azure.com/%23blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies)

*Note: This script will check for a security group: “****sgu-Exclude from CA****,“ and create one if it does not yet exist. You should populate this group with your emergency access*

*account(s).*

© Copyright 2019-2022,

18

Communicating upcoming changes

Always communicate policy changes to end users in advance, for example at a Staff meeting, and via email communication:

Attention Staff:

On Thursday, at 12 PM noon, we are going to disable legacy forms of authentication as we discussed, and start requiring you to use the Microsoft Authenticator app. You can obtain this app from the App Store on Apple devices or the Google Play store on Android.

Please note that we no longer support the use of legacy client applications. You will be expected to use modern, supported applications moving forward.

If you experience any other unexpected interruptions, please contact the helpdesk at: [Contact info here]

Thank you,

[Your Signature Here]

have some [customer communication templates](https://gumroad.com/vanvfields#BCxFF) available, including screen shots for end users to follow. Feel free to use and re-brand them as your own during your implementations.

© Copyright 2019-2022,

19



Global persona policies

Any policy leading with a “0” is assigned to **All users** (global persona). The following table lists the settings contained within the recommended custom policies. Policies which require you to specify named locations or terms of use are not included with my baseline script.

*1 These policies are included in my baseline script on GitHub*

*2 Always exclude at least one emergency access account*

© Copyright 2019-2022,

20

**Policy Name Assignments Conditions Access Control**

**CA001: Block legacy authentication**1

**Include Users:** All users2 **Cloud Apps:** All cloud apps

**Client apps Include**: EAS Clients, Other clients

**Block access**

**CA002: Block unsupported device platforms**1

**Include Users:** All users2 **Cloud Apps:** All cloud apps

**Device platforms**: **Include**: All devices **Exclude**: Select all (e.g., Windows, iOS, Android, MacOS)

**Block access**

**CA003: Require MFA for Azure Management**1

**Include Users:**

All users2

**Cloud Apps:** Azure Management

**Locations:**

**Include**: All locations **Exclude**: All trusted locations

**Block access**

**CA004: Require MFA to register or join devices**1

**Include Users**:

All users2

**User actions**:

Register or join devices

**None**

**Grant access:** Require multi-factor authentication

**CA005: No persistent browser session for unmanaged devices**

**Include Users:** All users2 **Cloud Apps:** All cloud apps

**Device filters**:

**Not equals:** Hybrid- joined or Compliant

**Session: Sign-in frequency: 2 hours,**

**+ Never persistent browser**

**CA006: Block unsupported sign-in countries**

**Include Users:** All users2 **Cloud Apps:** All cloud apps

**Locations:** All locations **Exclude**: Supported sign-in countries **Device filters**:

**Not equals:** Hybrid- joined or Compliant

**Block access**

**CA007: Terms of Use**

**Include Users:** All users2 **Cloud Apps:** All cloud apps

**None**

**Terms of use**



Admin persona policies

These policies target administrator roles.

*1 These policies are included in my baseline script on GitHub*

*2 Always exclude at least one emergency access account*

© Copyright 2019-2022,

21

**Policy name Assignments Conditions Access Controls**

**CA101: Require MFA for admins**1

**Include Users:** Select admin roles2 **Cloud Apps**:

All cloud apps

**None**

**Grant access:** Require multi-factor authentication

**CA102: No persistent browser for admins**

**Include Users:** Select admin roles2 **Cloud Apps**:

All cloud apps

**None**

**Session: Sign-in frequency: 1 hour, + Never persistent browser**

**CA103: Require managed devices for admins**

**Include Users:** Select admin roles2 **Cloud Apps**:

All cloud apps excluding Intune Enrollment, or at least Azure Management

**None**

**Grant access:** Require device to be marked as compliant



Internal persona policies

Internal persona policies target standard, internal users (e.g., employees) and as such we generally exclude guests and external users, and even administrator roles in some cases.

1 *These policies are included in my baseline script on GitHub*

2 *Exclude at least one emergency access account, plus guests and external users*

© Copyright 2019-2022,

22

**Policy Name Assignments Conditions Access Control**

**CA201: Require MFA or compliant device for internal users**1

**Include Users**: All users2 **Cloud Apps**: All cloud apps

**None**

**Grant access:** Require multi-factor authentication **OR** Require device to be marked as compliant

**CA202: Securing security info registration**1

**Include Users**: All users2

**User actions**:

Register security information

**None**

**Grant access:** Require multi-factor authentication

**CA203: Require MAM or MDM for mobile devices (Office 365)** 1

**Users:** All users2 **Cloud Apps:** Office 365

**Device platforms**: iOS and Android

**Grant access:**

Require approved client app **OR** Require app protection policy **OR** Require device to be marked as compliant

**CA204: Require managed devices for desktop client access (Office 365)** 1

**Users:** All users2 **Cloud Apps:** Office 365

**Device platforms**: Windows, macOS **Client apps**:

Mobile apps and desktop clients

**Grant access:**

Require device to be marked as compliant **OR** Require Hybrid Azure AD joined device

**CA205: Block downloads on unmanaged devices (Office 365)**

**Users:** All users2 **Cloud Apps:** Office 365

**None**

**Session:**

Use app enforced restrictions



Guest-specific policy examples

These policies are optional, and subject to the requirements of the business. It is a good practice to exclude guests from most policies and target them specifically with the policies you want them to have. Some policies that are applied to internal users simply would not be practical for guests, for example

you would not want to require guest devices to become enrolled and managed by your organization.

1 *These policies are included in my baseline script on GitHub*

2 *Exclude at least one emergency access account*

*Note: If you want to implement policies targeting guests which enforce access controls such as Multi-factor authentication and Compliant device, you should also plan to enable the* ***Cross-tenant access settings*** *from* ***External Identities*** *area. Specifically,* ***Default settings > Edit inbound defaults****, then choose* ***Trust settings****. Select all of*

*the options here to trust claims from other Azure AD tenants.*

© Copyright 2019-2022,

23

**Policy Name Assignments Conditions Access Control**

**CA301: Block guest access to unsupported apps**1

**Users:** Guests and external users2 **Cloud Apps:**

All cloud apps

**Exclude apps**: Office 365

**None**

**Block access**

**CA302: Require MFA for guests and external users**1

**Users:** Guests and external users2 **Cloud Apps:**

All cloud apps

**None**

**Grant access:** Require multi-factor authentication

**CA303: Require terms of use for guests**

**Users:** Guests and external users2 **Cloud Apps:**

All cloud apps

**None**

**Grant access:**

Terms of use for guest access



Service account policy examples

The final category of policies centers around service accounts. These are accounts which do not represent a real human like you and me, but rather a robot or automated process or application. The two most common use cases are below (limit which apps the account can interact with and limit the

locations from which the account can operate).

You can repeat these policies for as many service accounts or service principals as needed.

Conclusion

This concludes my best practices guidance on Conditional Access. You can implement additional policies as needed; the policies included herein are samples that come directly from my experience

implementing Conditional Access with customers in the field.feedback

Feel free to reach out at any time or drop

© Copyright 2019-2022,

24

**Policy Name Assignments Conditions Access Control**

**CA401: Block service account access to unsupported apps**

**Users or Workload identities:** <Select user> **Cloud Apps:**

All cloud apps

**Exclude apps**:

<only the apps needed>

**None**

**Block access**

**CA402: Block service account access from untrusted locations**

**Users or Workload identities:** <Select user or service principal> **Cloud Apps:**

All cloud apps

**Location:** All locations **Exclude**: <Trusted locations or Named locations from which the account operates>

**Block access**